DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-08384
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Julie R. Mendez, Esquire, Department Counsel
For Applicant: *Pro se*

November 28, 2011

Decision

RIVERA, Juan J., Administrative Judge:

Between 1997 and the summer of 2008, Applicant illegally downloaded digital material and accessed other people's computers and a wireless system without authorization. His immaturity led to his questionable behavior. He was forthcoming and candid during his security clearance interviews. He received training about ethical behavior and the handling of information technology systems. He expressed sincere remorse for his past questionable behavior and understands that it could adversely impact on his ability to hold a security clearance. His questionable behavior is unlikely to recur. Applicant mitigated security concerns under Guidelines E and M.

Statement of the Case

Applicant submitted a security clearance application on June 12, 2010. After reviewing the results of the ensuing background investigation, adjudicators for the Defense Office of Hearings and Appeals (DOHA) were unable to make a preliminary

affirmative finding[1] that it is clearly consistent with the national interest to grant Applicant's request for a security clearance. On June 15, 2011, DOHA issued Applicant a statement of reasons (SOR), alleging security concerns under Guideline E (Personal Conduct), and Guideline M (Use of Information Technology Systems) of the adjudicative guidelines (AG).[2]

On July 11, 2010, Applicant responded to the SOR allegations and requested a hearing before an administrative judge. The case was assigned to me on September 27, 2011. DOHA issued a notice of hearing on September 29, 2011, and the hearing was convened as scheduled on October 25, 2011. At the hearing, the Government offered exhibits (GE) 1 through 3, which were admitted without objection. Applicant testified, and he presented exhibits (AE) 1 through 11, which were admitted without objection. DOHA received the transcript of the hearing (Tr.) on November 2, 2011.

Findings of Fact

Applicant admitted all SOR allegations, with explanations, except for SOR ¶ 2.b. His admissions are incorporated herein as findings of fact. After a thorough review of the evidence of record, and having considered Applicant's demeanor and testimony, I make the following findings of fact.

Applicant is a 28-year-old information assurance associate working for a government contractor. He attended college from 2001 until 2006, and received a bachelor's degree in computer engineering technology. He completed his master's degree in information assurance in 2008. He married in July 2010, and has no children.

Since high school, Applicant has been a computer technology and software aficionado. As a teenager, he learned his skills by spending many hours playing with computers and software. He started illegally downloading computer software and music (digital material) in high school (around 1997), and continued to do so through college and until the summer of 2008. His illegal downloading of digital material diminished while he was in college and graduate school.

Applicant explained he had the mistaken belief that it was okay for him to illegally download digital material if he was not damaging anything or harming anyone. He illegally downloaded "tens of thousands of dollars" of digital material because he could not afford all the digital material he wanted to experiment with. Applicant claimed he did not profit from the illegal downloading of digital material. He only used the digital material for his personal use.

[1] Required by Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended; and Department of Defense (DoD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as revised.

[2] Adjudication of this case is controlled by the AGs, implemented by the DoD on September 1, 2006.

While in college, Applicant worked for his college's prestigious computer laboratory. In 2001-2002, he started working with government contractors through his college laboratory. Because of this job, he was granted a secret security clearance in 2002. In 2006, he started working for a different government contractor in support of another government agency. His access to classified information was upgraded to an interim top secret clearance in 2007. During his top secret security clearance interviews, Applicant was candid and disclosed the facts alleged in the SOR. His interim top secret clearance was revoked by the other government agency in May 2010.

In substance, Applicant disclosed that around 2000-2001, he remotely accessed seven computers without authorization from its owners by using Trojan Horse portals on the Internet. He explained that he did not infect the computers with the Trojan Horse software. He just took advantage of infected computers and used the Trojan Horse portals to access them. He denied that he ever damaged or stole anything from the systems he accessed. At his hearing, Applicant credibly testified that he now understands his actions were unethical and illegal. He promised never to engage in such actions again.

Between March and June 2008, without authorization, Applicant deliberately broke the encryption key of his neighbor's wireless signal. He experimented with his neighbor's secured wireless network because he was interested in learning about securing wireless networks. He wanted to know whether he could break the encryption key. After obtaining the encryption key, he confirmed it was valid, but he never accessed the neighbor's network or the wireless station.

Applicant explained he was immature and too eager to experiment with computers. He did not have the knowledge and training to understand the consequences of his actions. Applicant averred he did not realize his actions were illegal until he attended graduate school and took his first class covering intellectual property, trademarks, and copyright laws. That class forced him to reflect and reconsider his illegal downloading of digital material because of the possible adverse effect it could have on his ability to hold his job and a security clearance.

Since 2008, Applicant has received training from his employer about the ethical and legal rules covering the accessing of other people's computers and wireless systems. He learned that he must have permission to access other people's computer systems, and that there are "rules of engagement" that he must follow. To further his education, in May 2010, he completed a Certified Ethical Hacker course.

From around 2003 until June 2006, while employed by his college laboratory, Applicant took computer equipment and materials home. The manager of the information security group at his college laboratory confirmed that personnel working at the laboratory were allowed to take excess or obsolete computer equipment and material home. The manager provided a very favorable character recommendation for Applicant. He considers Applicant to be "a most reliable and trustworthy individual." In his opinion, Applicant is well respected by his supervisors and peers, and admired for

his knowledge, dedication, and judgment. He provided Applicant with his highest recommendation for a security clearance.

Applicant started working for his current employer, a government contractor in October 2008. He is now applying the skills he learned on his own in his current job as a computer vulnerabilities and systems penetrations tester. He works in a highly sensitive position of trust. Applicant submitted numerous character reference statements from supervisors and peers. A reading of these documents shows that Applicant disclosed to his employers and supervisors his prior misuse of licensed and copyrighted digital materials. Moreover, his references are impressed with Applicant's openness in discussing his past transgressions and willingness to teach young employees about the ethical and legal ramifications of such actions. Applicant is considered to be an exceptional employee who displays technical proficiency and excellent performance. He is honest, trustworthy, and reliable. He was lauded for his character, maturity, and judgment. He has established a reputation for knowing and applying sound security practices.

Applicant expressed sincere remorse for his past behavior. He has matured during the last three years. Because of his personal education efforts and the training he has received from his employers, he now understands the ethical and legal consequences of accessing other peoples' computer systems without authorization and illegally downloading digital materials. He is now married and holds an important fulltime position with a large government contractor. Because of his excellent performance, he was promoted to a manager position. He supervises junior employees and mentors them about the proper handling of information technology systems and to avoid the mistakes he made.

Policies

The President of the United States has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information. *Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988). The President has authorized the Secretary of Defense to grant eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended. The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These AGs are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's adjudicative goal is a fair, impartial, and commonsense decision. An administrative

judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, to reach his decision.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information. Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. *See also* Executive Order 12968 (Aug. 2, 1995), Section 3. Thus, nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any expressed or implied determination about Applicant's allegiance, loyalty, or patriotism. It is merely an indication that the Applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996); and ISCR Case 08-06605 at 3 (App. Bd. Feb. 4, 2010).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue [his or her] security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

The facts and circumstances raising security clearance concerns under Guidelines M and E are substantially the same, with some exceptions. For the sake of brevity, they will be articulated under the Guideline M discussion, and incorporated by reference into the discussions under Guideline E. Material exceptions will be discussed in the pertinent guideline.

Guideline M, Use of Information Technology Systems

AG ¶ 39 articulates the security concern about the misuse of information technology systems:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

Between 1997 and the summer of 2008, Applicant illegally downloaded digital material, and he accessed other people's computers and a wireless system without authorization. He accessed other's computers and broke into a private wireless network to test his ability to penetrate the network. Although he was able to break into the systems, he never infected, modified, or damaged the private systems.

Applicant was unaware his actions were illegal. He did not access or manipulate any personal information. He did not enter his neighbor's wireless network when he identified the "key" to entering that network. He believed that it was okay for him to illegally download digital material if he was not damaging anything or harming anyone in the process.

His actions raised security concerns under AG ¶ 40:

> (a) illegal or unauthorized entry into any information technology system or component thereof;
>
> (c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system; and
>
> (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations.

AG ¶ 41 provides three potentially applicable mitigating conditions to the use of information technology systems concern:

> (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available; and

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

I find that only AG ¶ 41(a) applies to the facts in this case. Applicant's last questionable behavior occurred in the summer of 2008. As such, it is temporally remote. Most of his questionable behavior occurred while he was in college. He accessed the computer systems to test his ability to penetrate the networks. He was playing with computers, experimenting, testing security programs, and testing his own abilities. He never modified or damaged the systems after breaking into them. Nor did he share this information with anyone else. Applicant mistakenly believed his actions were not illegal because of his lack of knowledge and maturity.

Applicant's circumstances have changed and his misuse of information technology systems is not likely to recur. He disclosed to his employers and supervisors his prior misuse of licensed and copyrighted digital materials. He openly discussed his past transgressions during his security clearance process, and he is using his experiences to teach young employees about the ethical and legal ramifications of such actions. He has established a reputation for knowing and applying sound security practices.

Applicant expressed sincere remorse for his past behavior. He has matured during the last three years. Because of his personal education efforts, the training he received from his employers, and the security clearance process, he now understands the ethical and legal consequences of his misconduct. Moreover, he also understands that such behavior could adversely impact on his ability to hold his job and a security clearance. He is currently married and holds an important fulltime position with a large government contractor. Because of his performance, he was promoted to a manager and supervisory position. AG ¶¶ 41(b) and (c) are not applicable to Applicant's behavior because his misuse was not minor and his conduct was intentional.

Guideline E, Personal Conduct

AG ¶ 15 explains why personal conduct is a security concern stating:

Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful

and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

Applicant's questionable behavior, as discussed under Guideline M, incorporated herein, also raise security concerns under AG ¶ 16:

> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing; and
>
> (c) credible adverse information in several adjudicative areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information.

AG ¶ 17 lists seven conditions that could potentially mitigate the personal conduct security concerns:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;
>
> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;

(f) the information was unsubstantiated or from a source of questionable reliability; and

(g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

For the same reasons discussed previously under Guideline M, incorporated herein, I find that AG ¶ 17 (c), (d), and (e) apply and mitigate the Guideline E security concern.

Concerning SOR ¶ 2.b, I find that Applicant was authorized by the laboratory manager, and the laboratory's practice, to take computer equipment and materials home. This allegation was not substantiated by the evidence.

Whole-Person Concept

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case, and under the whole-person concept. AG ¶ 2(c). For the same reasons discussed under Guideline M, incorporated herein, I find that Applicant's questionable behavior is unlikely to recur and it does not cast doubt on Applicant's current judgment, reliability, and trustworthiness.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by Section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline M:	FOR APPLICANT
Subparagraphs 1.a - 1.c:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraphs 2.a - 2.b:	For Applicant

Conclusion

In light of all the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant or continue eligibility for a security clearance for Applicant. Security clearance is granted.

_____

JUAN J. RIVERA
Administrative Judge